PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-292135
(43)Date of publication of application : 19.10.2001

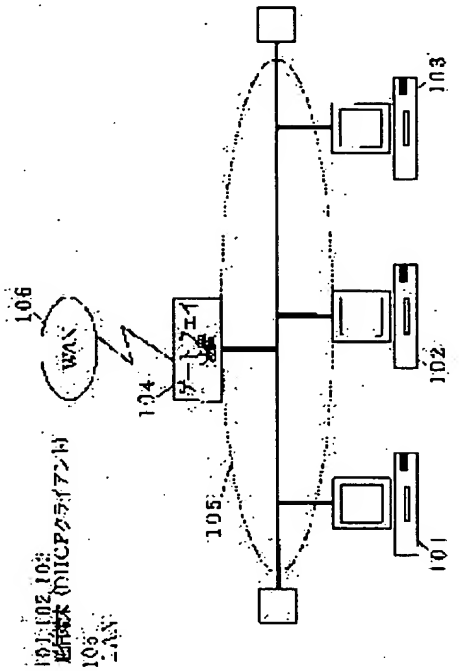
(51)Int.Cl. H04L 9/08
G09C 1/00
H04L 12/28
H04L 12/22

(21)Application number : 2000-106030
(22)Date of filing : 07.04.2000

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : MURAKAWA YASUSHI

(54) KEY EXCHANGE SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a key exchange system which can share password key data by allowing a plurality of communication terminals and a gateway device on a LAN to individually and easily exchange key data, by using an existing communication protocol.
SOLUTION: In the key exchange system, having a plurality of communication terminals 101, 102 and 103 connected to the LAN 105 and the gateway device 104 as a DHCP server, which is connected to the LAN and a WAN 106 and which performs concentration/conversion processing, the communication terminals 101, 102 and 103 exchange key data with the gateway device 104, in order to obtain network information at the time of starting DHCP communication.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－292135
（Ｐ２００１－２９２１３５Ａ）
(43)公開日　平成13年10月19日(2001.10.19)

(51)Int.Cl.[7]	識別記号	ＦＩ			テーマコード（参考）
H04L 9/08		G09C 1/00	660	E	5J104
G09C 1/00	660	H04L 9/00	601	C	5K030
H04L 12/28			601	E	5K033
12/22		11/00	310	D	9A001
		11/26			

審査請求　未請求　請求項の数４　ＯＬ　（全10頁）

(21)出願番号　特願2000－106030（Ｐ2000－106030）

(22)出願日　平成12年４月７日(2000.4.7)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

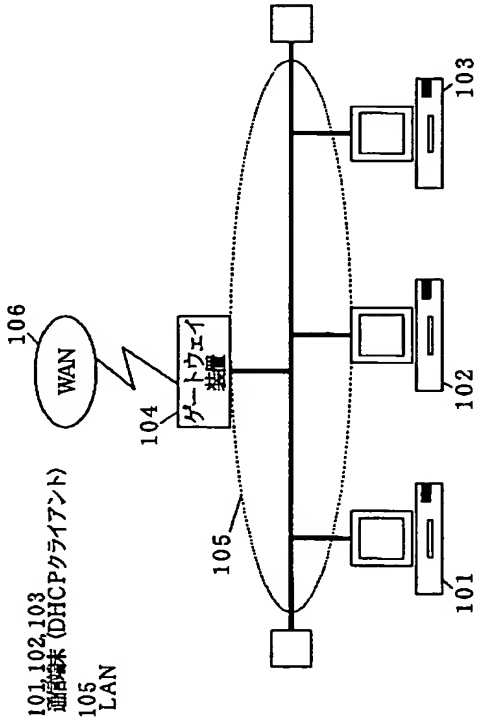
(72)発明者　村川　泰
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(74)代理人　100097445
弁理士　岩橋　文雄　（外２名）

最終頁に続く

(54)【発明の名称】鍵交換システム

(57)【要約】
【課題】　既存の通信プロトコルを利用して、ＬＡＮ上の複数台の通信端末とゲートウェイ装置とがそれぞれ別個に簡易に鍵データを交換することにより、暗号鍵データを共有することができる鍵交換システムを提供することを目的とする。
【解決手段】　ＬＡＮ１０５に接続された複数の通信端末１０１、１０２、１０３と、ＬＡＮおよびＷＡＮ１０６に接続され集線・変換処理を行うＤＨＣＰサーバとしてのゲートウェイ装置１０４とを有する鍵交換システムであって、通信端末１０１、１０２、１０３は、起動時にネットワーク情報を取得するためにゲートウェイ装置１０４との間で行うＤＨＣＰ通信時に、鍵データも同時に交換する。



1

【特許請求の範囲】

【請求項１】ＬＡＮに接続された複数の通信端末と、ＬＡＮおよびＷＡＮに接続され集線・変換処理を行うＤＨＣＰサーバとしてのゲートウェイ装置とを有する鍵交換システムであって、

前記通信端末は、起動時にネットワーク情報を取得するために前記ゲートウェイ装置との間で行うＤＨＣＰ通信時に、鍵データも同時に交換することを特徴とする鍵交換システム。

【請求項２】前記通信端末は、付与されたネットワーク情報の有効期限切れまでに前記ゲートウェイ装置に対して行うネットワーク情報の延長申請要求から始まるＤＨＣＰ通信時に、以前交換した共有鍵データを廃棄し、新たに鍵データを交換して共有鍵データを更新することを特徴とする請求項１に記載の鍵交換システム。

【請求項３】ＬＡＮに接続された複数の通信端末と、ＬＡＮおよびＷＡＮに接続され集線・変換処理を行うＤＨＣＰサーバとしてのゲートウェイ装置とを有する鍵交換システムであって、

前記通信端末は、前記ゲートウェイ装置を介してＷＡＮに送信されるデータについてのみ暗号鍵データで通信データを暗号化してＬＡＮに送信し、前記ゲートウェイ装置は、前記送信元の通信端末と共有する暗号鍵データを使用して通信データを復号化してＷＡＮに送信することを特徴とする鍵交換システム。

【請求項４】前記ゲートウェイ装置は、ＷＡＮからＬＡＮ内の宛先通信端末へのパケットを受信し、前記宛先通信端末と共有する暗号鍵データで通信データを暗号化してＬＡＮに出力し、前記宛先通信端末は、前記ゲートウェイ装置との間で共有する暗号鍵データを使用して復号化することを特徴とする請求項３に記載の鍵交換システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、複数の通信端末とその複数の通信端末を接続したＬＡＮとそのＬＡＮをインターネットなどのＷＡＮに接続するゲートウェイ装置とで構成され、しかもＬＡＮ内の各通信端末がＤＨＣＰ（Ｄｙｎａｍｉｃ Ｈｏｓｔ Ｃｏｎ－ｆｉｇｕｒａｔｉｏｎ Ｐｒｏｔｏｃｏｌ）クライアントとしてネットワーク情報を要求し、ゲートウェイ装置がＤＨＣＰサーバとして各通信端末にネットワーク情報を付与して一元管理するＬＡＮシステムにおいて、ＬＡＮ内通信の秘匿性を確保してＷＡＮとの通信を行う鍵交換システムに関するものである。

【０００２】

【従来の技術】近年、インターネットの爆発的に普及に伴い、企業のみならず家庭でもＬＡＮを構築する事例が増えている。また、マンションなどの集合住宅でＬＡＮを構築し、各家庭の端末からＬＡＮ経由でインターネットに接続するなど、これまでの企業で構築されてきたものとは性質の異なる形態のＬＡＮも登場している。こうした形態の場合、インターネットへの接続性のみが重視され、通常のＬＡＮで重要視される情報の共有は必要なくなり、逆にＬＡＮ内でのネットワーク情報の秘匿化が必要になる。また企業などで構築される既存のＬＡＮにおいても、共有する情報とは別にＬＡＮ内の通信データを暗号化して安全性を確保する需要が高まっている。

【０００３】図１は、ＬＡＮ内の通信データを暗号化して安全性を確保するための一般的な鍵交換システムを示す構成図である。

【０００４】図１において、１０１～１０３は後述のＬＡＮ１０５内の通信端末（例えばパソコン）、１０４はＬＡＮ１０５と後述のＷＡＮ１０６との間に介在し、集線・変換処理を行うゲートウェイ装置、１０５は通信端末１０１～１０３とゲートウェイ装置１０４とが接続されたＬＡＮ、１０６はインターネットなどのＷＡＮである。通信端末１０１～１０３およびゲートウェイ装置１０４がＬＡＮ１０５に出力したパケットデータは、ＬＡＮ１０５内に接続された全ての端末、つまり通信端末１０１～１０３とゲートウェイ装置１０４とが受信することになる。

【０００５】図２は、図１に示すゲートウェイ装置と通信端末を詳細に示すブロック図である。

【０００６】図２において、２０１はＬＡＮ２１０及びＷＡＮ２０９との間に介在して集線、変換処理を行うゲートウェイ装置であり、ゲートウェイ装置２０１は、ネットワークに接続するインタフェースとして、ＬＡＮ２１０に接続するＬＡＮ物理接続部と、ＷＡＮ２０９に接続するＷＡＮ物理接続部２０３とを持ち、その接続の制御をそれぞれＬＡＮコントローラ２０４とＷＡＮコントローラ２０５が行う。そして、ゲートウェイとしてのルーティング機能はルーティング処理部２０６が行うが、そのためにはネットワーク情報テーブル２０８を参照・登録する必要がある。このネットワーク情報テーブル２０８は記憶装置２０７の内部に構築される。２１１はＬＡＮ２１０を介して接続される通信端末２１１であり、通信端末１１は、ネットワークに接続するインタフェースとして、ＬＡＮ２１０と接続するＬＡＮ物理接続部２１２を持ち、ＬＡＮ物理接続部２１２の接続はＬＡＮコントローラ２１３により制御される。通信端末としての機能は通信プロトコル処理部２１４が行うが、そのためにはネットワーク情報テーブル２１６を参照・登録する必要がある。このネットワーク情報テーブル２１６は記憶装置２１５の内部に構築される。

【０００７】次に、ＤＨＣＰ通信モデルについて図３を参照しながら解説する。図３は通信端末としてのＤＨＣＰクライアント３０１とＤＨＣＰサーバ３０２との間の通信手順を示すシーケンス図である。図３において、３０１はＤＨＣＰクライアント、３０２はＤＨＣＰサーバ

である。ＤＨＣＰはライアント・サーバモデルの通信プロトコルで、ＤＨＣＰサーバ３０２がネットワーク内の通信端末３０１のＩＰアドレスなどのネットワーク情報を一元管理するためのメカニズムを提供する。一般的には、ＬＡＮ上のＤＨＣＰサーバ３０２が、同一セグメント内の通信端末３０１にＩＰアドレスなどのネットワーク情報を有効期限付きで付与する形で利用される。

【０００８】図３において、まず、通信端末３０１は、電源起動後にＩＰアドレス構築のため、ＬＡＮ内の全端末に向けてＤＨＣＰＤＩＳＣＯＶＥＲメッセージをブロードキャスト（同報通信）する（Ｓ１）。ＤＨＣＰＤＩＳＣＯＶＥＲメッセージを受信したネットワーク内のＤＨＣＰサーバ３０２は、要求された構成情報をＤＨＣＰＯＦＦＥＲメッセージにより通知する（Ｓ２）。ネットワーク上に複数のＤＨＣＰサーバが存在する場合、その全てがＤＨＣＰＯＦＦＥＲメッセージを送信し、ＤＨＣＰクライアント３０１は複数のＤＨＣＰＯＦＦＥＲメッセージを受信することになる。

【０００９】ＤＨＣＰＯＦＦＥＲメッセージを受信したＤＨＣＰクライアント３０１は、複数のＤＨＣＰサーバからメッセージを受信した場合は図３ではＤＨＣＰサーバ３０２を選択し、選択したＤＨＣＰサーバ３０２にＤＨＣＰＲＥＱＵＥＳＴメッセージを送信し、ＩＰアドレス他のネットワーク情報を要求する（Ｓ３）。対するＤＨＣＰサーバ３０２は、ＤＨＣＰクライアント３０１からの要求が妥当でそれに応えられる場合は、ＤＨＣＰＡＣＫメッセージをＤＨＣＰクライアント３０１に送信し、ＩＰアドレスを含むネットワーク情報を付与し、ＤＨＣＰクライアント３０１はＩＰ通信が可能になる（Ｓ４）。また、この時ネットワーク情報の有効期限も設定される。ＤＨＣＰクライアント３０１は、この有効期限内（ＤＨＣＰの初期設定では有効期間の５０％の時間が経過した時点）にＤＨＣＰサーバ３０２にＩＰアドレス延長申請としてＤＨＣＰＲＥＱＵＥＳＴメッセージを送信し（Ｓ５）、ＤＨＣＰサーバ３０２はこれに対して返信することで（Ｓ６）、ネットワーク情報の更新・有効期限延長が行われる。

【００１０】次に、通信データの暗号化等で安全性を確保する既存のセキュリティ・プロトコルについて解説する。既存のセキュリティ・プロトコルとして代表的なものにＩＰｓｅｃ（Ｓｅｃｕｒｉｔｙ　ｆｏｒ　Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）やＰＧＰ（Ｐｒｅｔｔｙ　Ｇｏｏｄ　Ｐｒｉｖａｃｙ）などが存在するが、前者はパケットにおけるＩＰ層以降の暗号化／認証を提供するもので、主にゲートウェイ装置に実装され、ＷＡＮ上におけるＶＰＮ確立に利用されている。暗号鍵の管理は、手動鍵管理方式と自動鍵管理方式がある。自動鍵管理方式を実現するためには、ＩＫＥ（Ｉｎｔｅｒｎｅｔ　Ｋｅｙ　Ｅｘｃｈａｎｇｅ）というＩＰｓｅｃ本体とは別にプロトコルを実装しなければならない。後者ＰＧＰは電子メールの暗号化のみに用いられる。電子メールの暗号化／復号化には公開鍵暗号方式が用いられる。これは利用者が予め自分の公開鍵を鍵サーバに登録しておく。メールの送信者は鍵サーバから送り先の相手の公開鍵を取得し、それを用いてメール内容を暗号化し、送信する。メールの受信者は自分が所有する秘密鍵を用いて暗号化されたメールを復号化する。

【００１１】

【発明が解決しようとする課題】しかしながら、上記従来の鍵交換システムでは、ＬＡＮ内の通信のみを秘匿化することを目的にした通信プロトコルがなく、また２点間で通信データの暗号化／復号化を行う鍵データを共有させることが必要になるが、手動で２点間の鍵データを設定するのは非常に非効率的であるし、自動的に鍵データを共有させるためにも、鍵データ交換を行う通信プロトコルの実装、もしくはそれをサポートした製品の購入が必要となる。

【００１２】この鍵交換システムでは、既存の通信プロトコルを利用して、ＬＡＮ上の複数台の通信端末とゲートウェイ装置とがそれぞれ別個に簡易に鍵データを交換することにより、暗号鍵データを共有することが要求されている。

【００１３】本発明は、この要求を満たすため、既存の通信プロトコルを利用して、ＬＡＮ上の複数台の通信端末とゲートウェイ装置とがそれぞれ別個に簡易に鍵データを交換することにより、暗号鍵データを共有することができる鍵交換システムを提供することを目的とする。

【００１４】

【課題を解決するための手段】この課題を解決するために本発明の鍵交換システムは、ＬＡＮに接続された複数の通信端末と、ＬＡＮおよびＷＡＮに接続され集線・変換処理を行うＤＨＣＰサーバとしてのゲートウェイ装置とを有する鍵交換システムであって、通信端末は、起動時にネットワーク情報を取得するためにゲートウェイ装置との間で行うＤＨＣＰ通信時に、鍵データも同時に交換する構成を備えている。

【００１５】この構成により、既存の通信プロトコルを利用して、ＬＡＮ上の複数台の通信端末とゲートウェイ装置とがそれぞれ別個に簡易に鍵データを交換することにより、暗号鍵データを共有することができる鍵交換システムが得られる。

【００１６】

【発明の実施の形態】本発明の請求項１に記載の鍵交換システムは、ＬＡＮに接続された複数の通信端末と、ＬＡＮおよびＷＡＮに接続され集線・変換処理を行うＤＨＣＰサーバとしてのゲートウェイ装置とを有する鍵交換システムであって、通信端末は、起動時にネットワーク情報を取得するためにゲートウェイ装置との間で行うＤＨＣＰ通信時に、鍵データも同時に交換することとしたものである。

【００１７】この構成により、ゲートウェイ装置と各通信端末との間でそれぞれ別個に、２点間で共有鍵暗号方式によって通信データの暗号化／復号化を行う際に使用できる鍵データが簡易に共有されるという作用を有する。

【００１８】請求項２に記載の鍵交換システムは、請求項１に記載の鍵交換システムにおいて、通信端末は、付与されたネットワーク情報の有効期限切れまでにゲートウェイ装置に対して行うネットワーク情報の延長申請要求から始まるＤＨＣＰ通信時に、以前交換した共有鍵データを廃棄し、新たに鍵データを交換して共有鍵データを更新することとしたものである。

【００１９】この構成により、ＬＡＮ内部で定期的に行われるＤＨＣＰセッションと鍵データ交換手順を同期させ、ＬＡＮ内の各通信端末とゲートウェイ装置で共有する暗号鍵データの定期的な更新を確立し、暗号鍵データの安全性を向上させるという作用を有する。

【００２０】請求項３に記載の鍵交換システムは、ＬＡＮに接続された複数の通信端末と、ＬＡＮおよびＷＡＮに接続され集線・変換処理を行うＤＨＣＰサーバとしてのゲートウェイ装置とを有する鍵交換システムであって、通信端末は、ゲートウェイ装置を介してＷＡＮに送信されるデータについてのみ暗号鍵データで通信データを暗号化してＬＡＮに送信し、ゲートウェイ装置は、送信元の通信端末と共有する暗号鍵データを使用して通信データを復号化してＷＡＮに送信することとしたものである。

【００２１】この構成により、ＷＡＮへの送信性を損なうことなくＬＡＮ内の通信のみを暗号化して秘匿化が実現されるという作用を有する。

【００２２】請求項４に記載の鍵交換システムは、請求項３に記載の鍵交換システムにおいて、ゲートウェイ装置は、ＷＡＮからＬＡＮ内の宛先通信端末へのパケットを受信し、宛先通信端末と共有する暗号鍵データで通信データを暗号化してＬＡＮに出力し、宛先通信端末は、ゲートウェイ装置との間で共有する暗号鍵データを使用して復号化することとしたものである。

【００２３】この構成により、ＷＡＮからの受信性を損なうことなくＬＡＮ内の通信のみを暗号化して秘匿化が実現されるという作用を有する。

【００２４】以下、本発明の実施の形態について図１～図１０を用いて説明する。

【００２５】（実施の形態１）本発明の実施の形態１による鍵交換システムの構成は図１、図２と同様であるので、その説明は省略する。本実施の形態と従来の技術とが異なるところは、ゲートウェイ装置としてのＤＨＣＰサーバとパソコン等の通信端末（ＤＨＣＰクライアント）の機能、動作等に関する点である。

【００２６】このような構成の鍵交換システムについて、図１、図３～図８を用いて説明する。図４（ａ）、（ｂ）はＤＨＣＰ通信によって付与されるデータの詳細を示すデータ図であり、図４（ａ）はＤＨＣＰデータ構造の詳細を示し、図４（ｂ）はＤＨＣＰサーバから付与される主なネットワーク情報の項目を示す。また、図５はＤｉｆｆｉｅ－Ｈｅｌｌｍａｎ方式による鍵交換の説明図であり、図６は一方の通信端末Ａの動作を示すフローチャート、図７は他方の通信端末Ｂの動作を示すフローチャート、図８はＤＨＣＰクライアントとしての通信端末とＤＨＣＰサーバとしてのゲートウェイ装置との間の通信シーケンスを示すシーケンス図である。図８において、６０１はＤＨＣＰクライアントとなる通信端末、６０２はＤＨＣＰサーバとなるゲートウェイ装置である。

【００２７】図１において、ＬＡＮ１０５に接続する通信端末１０１～１０３は、起動時に図４（ｂ）に列挙したネットワーク情報を取得するために、ＤＨＣＰサーバであるゲートウェイ装置１０４とＤＨＣＰ通信を行う。この際に同時に、図４（ａ）のＤＨＣＰメッセージにおけるオプションフィールド（オプション部）を利用し、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ（ディッフィー・ヘルマン）の鍵交換方式によって、通信端末１０１～１０３とゲートウェイ装置１０４との間で個別に暗号鍵を共有する。

【００２８】図５において、Ａ、ＢはＤｉｆｆｉｅ－Ｈｅｌｌｍａｎ方式を用いて鍵交換を行う通信端末で、まず鍵交換を始める前に、通信端末Ａ、Ｂ間であらかじめ素数であるｐと、１＜α＜ｐとなる適当な整数αを決めておく必要がある。ｐとαはＡ、Ｂ以外の第三者に知られてもよい。次に、通信端末Ａは適当な正の整数Ｘａを選び、図６に示すように（数１）を計算し（Ｓ１１）、鍵データＹａをＢに送信する（Ｓ１２）（なお、ｍｏｄとは割り算の剰余の表現のことであり、例えば１７ｍｏｄ　７とは１７を７で割った余りのことである）。

【００２９】

【数１】

$$Ya=\alpha^{Xa} \bmod p$$

【００３０】この時、通信端末Ａ以外の他者にＸａを知られてはいけない（Ｘａは秘密鍵といわれる）。同様に通信端末Ｂは適当な正の整数Ｘｂを選び、図７に示すように（数２）を計算し（Ｓ２１）、鍵データＹｂをＡに送信する（Ｓ２２）。

【００３１】

【数２】

$$Yb=\alpha^{Xb} \bmod p$$

【００３２】Ｘａと同様にＸｂも通信端末Ｂ以外の他者に知られてはならない（Ｘｂは秘密鍵データといわれる）。通信端末Ａは、通信端末Ｂから受信したＹｂを使用して、（数３）を計算し（Ｓ１３）、共有鍵データＫａｂを求めることができる。

【００３３】
【数３】

$$Kab=Yb^{Xa} \bmod p$$
$$=\alpha^{XaXb} \bmod p$$

【００３４】また通信端末Ｂも、（数４）を計算することで同様に共有鍵データＫａｂを求めることができる（Ｓ２３）。

【００３５】
【数４】

$$Kab=Ya^{Xb} \bmod p$$
$$=\alpha^{XaXb} \bmod p$$

【００３６】次に、ＤＨＣＰ通信とＤｉｆｆｉｅ－Ｈｅｌｌｍａｎ方式とを組み合わせた鍵交換システムについて図８で説明する。

【００３７】ＤＨＣＰクライアント６０１は起動時、ＩＰアドレスなどのネットワーク情報を取得するため、ＤＨＣＰＤＩＳＣＯＶＥＲメッセージをＬＡＮ内にブロードキャストする（Ｓ３１）。ＤＨＣＰＤＩＳＣＯＶＥＲメッセージを受信したＤＨＣＰサーバ６０２は、素数ｐと１＜α＜ｐとなる適当な正の整数αを決定し、ＤＨＣＰデータ構造におけるオプション部（図４（ａ）参照）に格納し、ＤＨＣＰＯＦＦＥＲメッセージとして返信する（Ｓ３２）。ｐ、αは第三者に知られてもよい情報なので、平文（ＤＨＣＰ通信における通常の文章データ）のまま通信路にのせても問題ない。

【００３８】ＤＨＣＰＯＦＦＥＲメッセージを受信したＤＨＣＰクライアント６０１は、ｐとαを受信する。もしＬＡＮ内に複数のＤＨＣＰサーバが存在していても、ＤＨＣＰデータのオプション部にｐとαが格納されているかどうかでＤＨＣＰサーバを選択可能である。通信端末６０１は適当な正の整数である秘密鍵データＸａを決定し、鍵データＹａを算出する。

【００３９】また同様にゲートウェイ装置５０２も、適当な正の整数である秘密鍵データＸｂを決定し、鍵データＹｂを算出する。ＤＨＣＰサーバを決定したＤＨＣＰクライアント６０１は、ＤＨＣＰＲＥＱＵＥＳＴメッセージを送信し（Ｓ３３）、ネットワーク情報をＤＨＣＰサーバ６０２に要求するが、このときＤＨＣＰデータのオプション部に独自に算出したＹａを格納しておく。

【００４０】ＤＨＣＰＲＥＱＵＥＳＴメッセージを受信したＤＨＣＰサーバ６０２は、通信端末６０１に付与するネットワーク情報をＤＨＣＰＡＣＫメッセージに格納し、返信する（Ｓ３４）。このとき独自に算出しておいたＹｂもＤＨＣＰデータのオプション部に格納しておく。ここに至ってＤＨＣＰクライアント６０１、ＤＨＣＰサーバ６０２の両者とも共有鍵データＫａｂを算出可能であり、通信端末６０１とゲートウェイ装置６０２との間で、通信データの暗号化／復号化を行う鍵データを安全に交換・共有できたことになる。

【００４１】以上のように本実施の形態では、通信端末６０１は、起動時にネットワーク情報を取得するためにゲートウェイ装置６０２との間で行うＤＨＣＰ通信時に、鍵データＹａ、Ｙｂも同時に交換するようにしたことにより、ゲートウェイ装置６０２と各通信端末６０１との間でそれぞれ別個に、２点間で共有鍵暗号方式によって通信データの暗号化／復号化を行う際に使用できる鍵を簡易に共有することができる。

【００４２】（実施の形態２）本発明の実施の形態２による鍵交換システムの構成は図１、図２と同様であるので、その説明は省略する。本実施の形態と従来の技術とが異なるところは、ゲートウェイ装置としてのＤＨＣＰサーバとパソコン等の通信端末の機能、動作等に関する点である。

【００４３】このような構成の鍵交換システムについて、図１、図４、図８を用いて説明する。

【００４４】図４（ｂ）に示すように、ＤＨＣＰ通信によって付与されるデータには、ＩＰアドレスやネットマスクの他に、付与したネットワーク情報の有効期限（貸し出し有効期限）というものがあり、ＤＨＣＰクライアントは付与された有効期限内（初期設定では有効期限の５０％）にＤＨＣＰサーバと通信し、ネットワーク情報の再取得を行う。図３に示すように、ネットワーク情報の再取得は、ＤＨＣＰＤＩＳＣＯＶＥＲ、ＤＨＣＰＯＦＦＥＲメッセージの送受信は必要なく、ＤＨＣＰＲＥＱＵＥＳＴ、ＤＨＣＰＡＣＫメッセージの送受信のみで行われる（ステップＳ５、Ｓ６参照）。ネットワーク情報の再取得に関しては、ＩＰアドレスなど以前取得した情報を基本的にはできる限りそのまま保持する形で行われるが、共有鍵データはネットワーク情報再取得の際に内容を更新するようにして、共有鍵データの安全性を高める。

【００４５】このような共有鍵データの更新について、ネットワーク情報再取得時の鍵情報更新手順を示す図８を用いて説明する。

【００４６】図８に示すように、ネットワーク再取得のトリガがＤＨＣＰクライアント６０１にかかると、以前使用した秘密鍵データＸａを廃棄し、新たに正の整数である秘密鍵データＸａを再設定し、鍵データＹａを算出する。そして、ＤＨＣＰサーバ６０２に対してＤＨＣＰＲＥＱＵＥＳＴメッセージを送信する（Ｓ３５）。この際、ＤＨＣＰデータのオプション部に再計算した鍵データＹａを格納しておく。ＤＨＣＰクライアント６０１からのＤＨＣＰＲＥＱＵＥＳＴメッセージを受信したＤＨＣＰサーバ６０２は、以前使用した秘密鍵データＸｂを廃棄し、新たに正の整数である秘密鍵データＸｂを再設定し、鍵データＹｂを算出する。そして、ＤＨＣＰクライアント６０１に対してネットワーク情報を付与するＤＨＣＰＡＣＫメッセージを送信するが（Ｓ３６）、ＤＨＣＰデータのオプション部に鍵データＹｂを格納しておく。ここに至ってＤＨＣＰクライアント（通信端末）６

０１、ＤＨＣＰサーバ（ゲートウェイ装置）６０２の両者とも新しい共有鍵データＫａｂを算出可能であり、通信端末６０１とゲートウェイ装置６０２の間で通信データの暗号化／復号化を行う鍵を更新できたことになる。

【００４７】以上のように本実施の形態では、通信端末６０１は、付与されたネットワーク情報の有効期限切れまでにゲートウェイ装置６０２に対して行うネットワーク情報の延長申請要求から始まるＤＨＣＰ通信時に、以前交換した共有鍵データを廃棄し、新たに鍵データを交換して共有鍵データを更新するようにしたことにより、ＬＡＮ内部で定期的に行われるＤＨＣＰセッションと鍵交換手順を同期させ、ＬＡＮ内の各通信端末６０１とゲートウェイ装置６０２で共有する暗号鍵データの定期的な更新を確立して、暗号鍵データの安全性を向上させることができる。

【００４８】（実施の形態３）本発明の実施の形態３による鍵交換システムの構成は図１、図２と同様であるので、その説明は省略する。本実施の形態と従来の技術とが異なるところは、ゲートウェイ装置としてのＤＨＣＰサーバとパソコン等の通信端末の機能、動作等に関する点である。

【００４９】このような構成の鍵交換システムについて、図９、図１０を用いて説明する。図９はＬＡＮ内における暗号化通信のイメージ図であり、図１０（ａ）は通信端末７０１が保持するネットワーク情報と鍵情報の管理テーブルを示すテーブル図、図１０（ｂ）はゲートウェイ装置７０４が保持するネットワーク情報と鍵情報の管理テーブルを示すテーブル図である。

【００５０】図９において、７０１～７０３は後述のＬＡＮ７０９内の通信端末、７０４はゲートウェイ装置、７０５はインターネットなどのＷＡＮ、７０６、７０７、７０８はゲートウェイ装置７０４と通信端末７０１、通信端末７０２、通信端末７０３との間で暗号鍵データ（それぞれＫ１、Ｋ２、Ｋ３）を共有することで構築されるＶＰＮ、７０９はＬＡＮである。

【００５１】図９において、通信端末７０１がＷＡＮ７０５に向けてパケットを送信する場合、ゲートウェイ装置７０４がパケットを中継（ルーティング）する。通信端末７０１は、保持するネットワーク情報と鍵情報の管理テーブルをみると、ゲートウェイ装置７０４との間で暗号鍵データＫ１を共有しているので、暗号鍵データＫ１を用いてパケットを暗号化し、ＬＡＮ７０９上に送信する。通信端末７０１からゲートウェイ装置７０４へのパケットはＬＡＮ７０９に接続する全端末が受信可能であるが、通信端末７０１とゲートウェイ装置７０４の２点間のみで共有される暗号鍵データＫ１で暗号化されているため、通信端末７０１とゲートウェイ装置７０４との間で構築されたＶＰＮ７０６上を流れているものとみなすことが可能である。暗号化済みパケットを受信したゲートウェイ装置７０４は、パケットの送信元ＭＡＣアドレスを保持するネットワーク情報と鍵情報の管理テーブルで検索し、暗号鍵データＫ１により暗号化されていることが分かるので、共有暗号鍵データＫ１でパケットを復号化し、ＷＡＮ７０５にパケットを送信する。

【００５２】また、逆にＷＡＮ７０５からＬＡＮ７０９内の通信端末７０１宛てのパケットをゲートウェイ装置７０４が受信した場合、宛先のＩＰアドレスと保持するネットワーク情報、鍵情報管理テーブルで検索し、宛先が通信端末７０１であることと通信端末７０１との間で暗号鍵データＫ１を共有していることが分かる。そこで、ゲートウェイ装置７０４は、暗号鍵データＫ１を使用してパケットを暗号化し、ＬＡＮ７０９に送信する。通信端末７０１は、宛先ＭＡＣアドレスが自身のものであるので、送信元のＭＡＣアドレスを保持するネットワーク情報、鍵情報管理テーブルで検索し、暗号鍵データＫ１を共有しているので、暗号鍵データＫ１を用いてパケットを復号化する。通信端末７０２、７０３も通信端末７０１宛てのパケットを受信することはできるが、暗号化／復号化鍵が異なるので正しく復号はできず、通信端末７０１とゲートウェイ装置７０４との間で構築されたＶＰＮ７０６上をデータが流れているものと考えることができる。以上のようにして、ＬＡＮ７０９内の上り／下りの両方についてデータの秘匿化を実現することが出来る。

【００５３】以上のように本実施の形態では、通信端末７０１は、ゲートウェイ装置７０４を介してＷＡＮ７０５に送信されるデータについてのみ暗号鍵データで通信データを暗号化してＬＡＮ７０９に送信し、ゲートウェイ装置７０４は、送信元の通信端末７０１と共有する暗号鍵データＫ１を使用して通信データを復号化してＷＡＮ７０５に送信するようにしたことにより、ＷＡＮ７０５への送信性を損なうことなくＬＡＮ７０９内の通信のみを暗号化して秘匿化を実現することができる。

【００５４】また、ゲートウェイ装置７０４は、ＷＡＮ７０５からＬＡＮ７０９内の宛先通信端末７０１へのパケットを受信し、宛先通信端末７０１と共有する暗号鍵データＫ１で通信データを暗号化してＬＡＮ７０９に出力し、宛先通信端末７０１は、ゲートウェイ装置７０４との間で共有する鍵データを使用して復号化するようにしたことにより、ＷＡＮ７０５からの受信性を損なうことなくＬＡＮ７０９内の通信のみを暗号化して秘匿化を実現することができる。

【００５５】

【発明の効果】以上説明したように本発明の請求項１に記載の鍵交換システムによれば、ＬＡＮに接続された複数の通信端末と、ＬＡＮおよびＷＡＮに接続され集線・変換処理を行うＤＨＣＰサーバとしてのゲートウェイ装置とを有する鍵交換システムであって、通信端末は、起動時にネットワーク情報を取得するためにゲートウェイ装置との間で行うＤＨＣＰ通信時に、鍵データも同時に

交換することにより、ゲートウェイ装置と各通信端末との間でそれぞれ別個に、２点間で共有鍵暗号方式によって通信データの暗号化／復号化を行う際に使用できる鍵データを簡易に共有することができるという有利な効果が得られる。

【００５６】請求項２に記載の鍵交換システムによれば、請求項１に記載の鍵交換システムにおいて、通信端末は、付与されたネットワーク情報の有効期限切れまでにゲートウェイ装置に対して行うネットワーク情報の延長申請要求から始まるＤＨＣＰ通信時に、以前交換した共有鍵データを廃棄し、新たに鍵データを交換して共有鍵データを更新することにより、ＬＡＮ内部で定期的に行われるＤＨＣＰセッションと鍵データ交換手順を同期させ、ＬＡＮ内の各通信端末とゲートウェイ装置で共有する暗号鍵データの定期的な更新を確立し、暗号鍵データの安全性を向上させることができるという有利な効果が得られる。

【００５７】請求項３に記載の鍵交換システムによれば、ＬＡＮに接続された複数の通信端末と、ＬＡＮおよびＷＡＮに接続され集線・変換処理を行うＤＨＣＰサーバとしてのゲートウェイ装置とを有する鍵交換システムであって、通信端末は、ゲートウェイ装置を介してＷＡＮに送信されるデータについてのみ暗号鍵データで通信データを暗号化してＬＡＮに送信し、ゲートウェイ装置は、送信元の通信端末と共有する暗号鍵データを使用して通信データを復号化してＷＡＮに送信することにより、ＷＡＮへの送信性を損なうことなくＬＡＮ内の通信のみを暗号化して秘匿化を実現することができるという有利な効果が得られる。

【００５８】請求項４に記載の鍵交換システムによれば、請求項３に記載の鍵交換システムにおいて、ゲートウェイ装置は、ＷＡＮからＬＡＮ内の宛先通信端末へのパケットを受信し、宛先通信端末と共有する暗号鍵データで通信データを暗号化してＬＡＮに出力し、宛先通信端末は、ゲートウェイ装置との間で共有する暗号鍵データを使用して復号化することにより、ＷＡＮからの受信性を損なうことなくＬＡＮ内の通信のみを暗号化して秘匿化を実現することができるという有利な効果が得られる。

【図面の簡単な説明】

【図１】一般的な鍵交換システムを示す構成図

【図２】図１に示すゲートウェイ装置と通信端末を詳細に示すブロック図

【図３】通信端末としてのＤＨＣＰクライアントとゲートウェイ装置としてのＤＨＣＰサーバとの間の通信手順を示すシーケンス図

【図４】（ａ）ＤＨＣＰ通信によって付与されるデータの詳細を示すデータ図

（ｂ）ＤＨＣＰ通信によって付与されるデータの詳細を示すデータ図

【図５】Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ方式による鍵交換の説明図

【図６】一方の通信端末の動作を示すフローチャート

【図７】他方の通信端末Ｂの動作を示すフローチャート

【図８】ＤＨＣＰクライアントとしての通信端末とＤＨＣＰサーバとしてのゲートウェイ装置との間の通信シーケンスを示すシーケンス図

【図９】ＬＡＮ内における暗号化通信のイメージ図

【図１０】（ａ）通信端末が保持するネットワーク情報と鍵情報の管理テーブルを示すテーブル図

（ｂ）ゲートウェイ装置が保持するネットワーク情報と鍵情報の管理テーブルを示すテーブル図

【符号の説明】

１０１、１０２、１０３、２１１、３０１、６０１、７０１、７０２、７０３通信端末（ＤＨＣＰクライアント）

１０４、２９１、３０２、６０２、７０４　ゲートウェイ装置（ＤＨＣＰサーバ）

１０５、２１０、７０９　ＬＡＮ

１０６、２０９、７０５　ＷＡＮ

２０２、２１２　ＬＡＮ物理接続部

２０３　ＷＡＮ物理接続部

２０４、２１３　ＬＡＮコントローラ

２０５　ＷＡＮコントローラ

２０６　ルーティング処理部

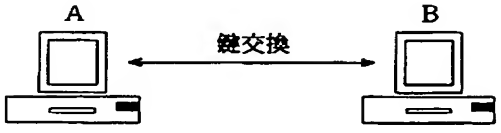
２０７、２１５　記憶装置

２０８、２１６　ネットワーク情報テーブル

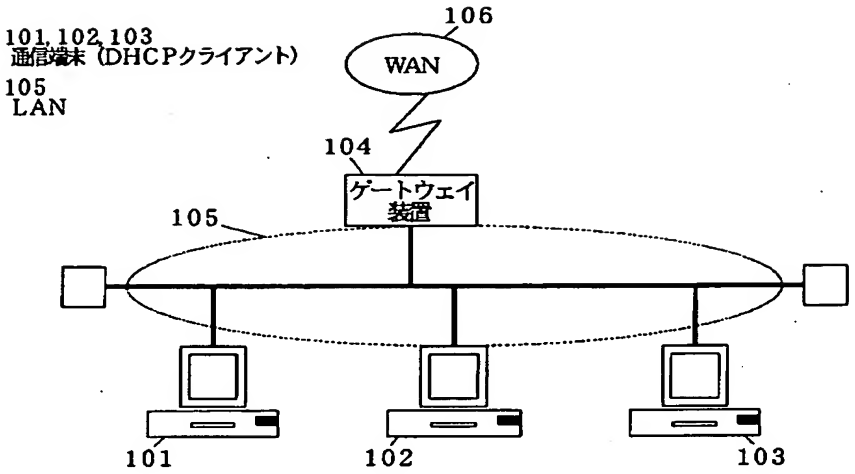
２１４　通信プロトコル処理部

７０６、７０７、７０８　ＶＰＮ

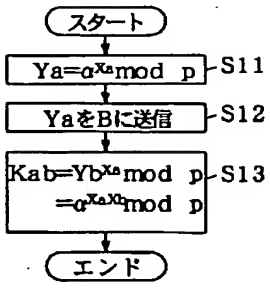
【図５】



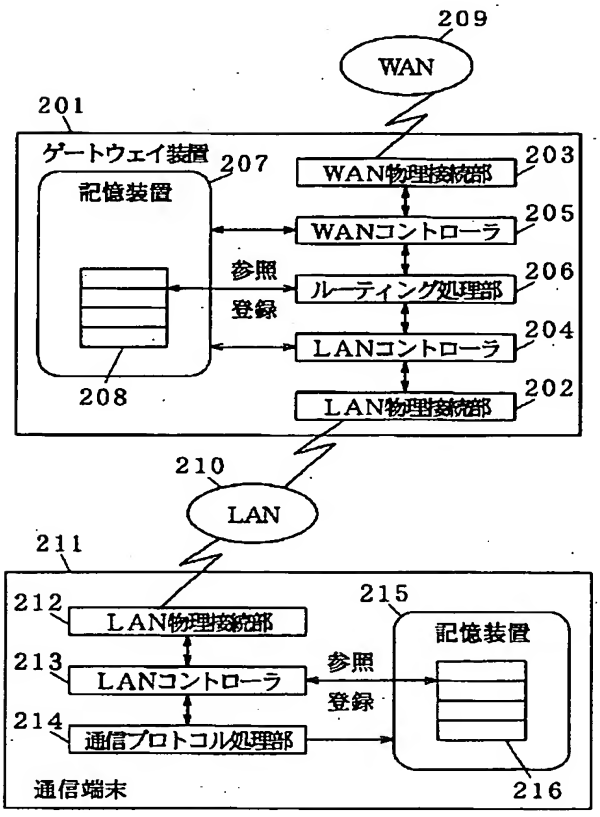
【図１】


101,102,103
通信端末（DHCPクライアント）
105
LAN
106
WAN
104
ゲートウェイ装置
105
101
102
103

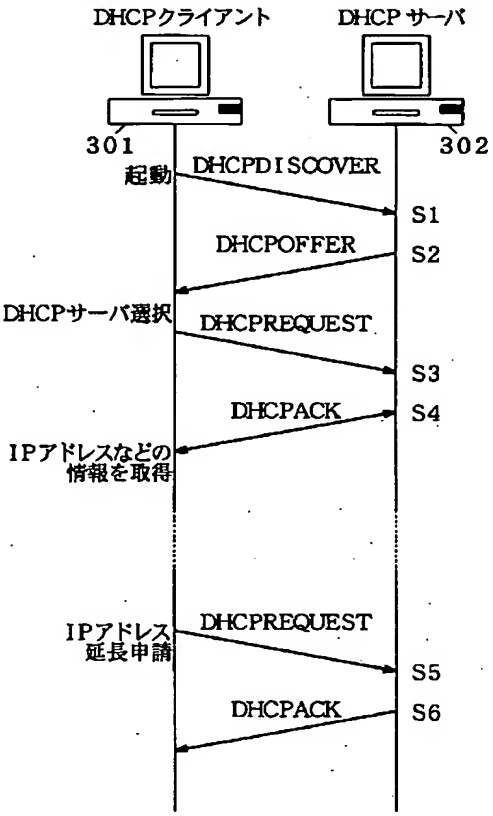
【図６】


スタート
Ya=α^Xa mod p
S11
YaをBに送信
S12
Kab=Yb^Xa mod p
=α^XaXb mod p
S13
エンド

【図２】


209
WAN
201
ゲートウェイ装置
207
記憶装置
WAN物理接続部
203
WANコントローラ
205
参照
登録
ルーティング処理部
206
LANコントローラ
204
208
LAN物理接続部
202
210
LAN
211
212
LAN物理接続部
215
記憶装置
213
LANコントローラ
参照
登録
214
通信プロトコル処理部
通信端末
216

【図３】


DHCPクライアント
DHCP サーバ
301
302
起動
DHCPDISCOVER
S1
DHCPOFFER
S2
DHCPサーバ選択
DHCPREQUEST
S3
DHCPACK
S4
IPアドレスなどの
情報を取得
IPアドレス
延長申請
DHCPREQUEST
S5
DHCPACK
S6

【図４】

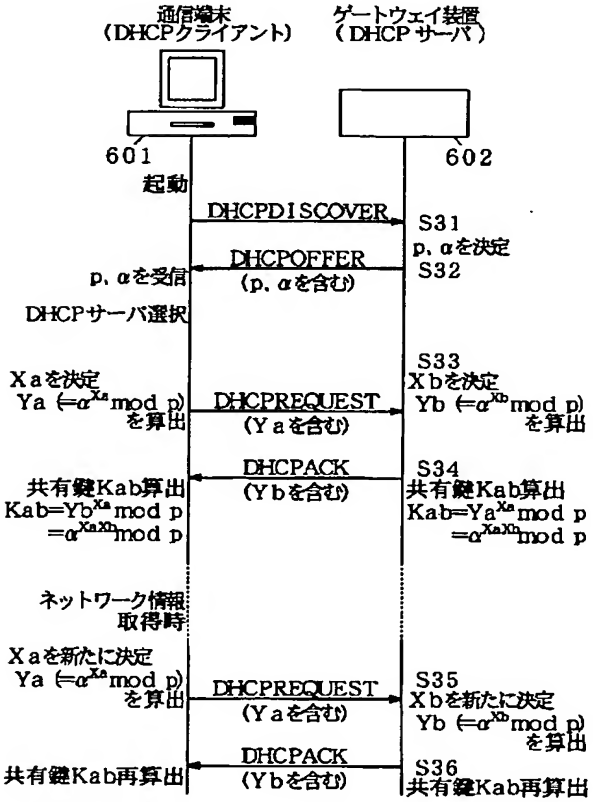
（ａ）

operation code(1)	ハードウェア番号(1)	ハードウェアアドレス長(1)	転送回数(1)
トランザクションＩＤ(4)			
経過時間(2)		ブロードキャスト・フラグ(2)	
クライアントＩＰアドレス(4)			
要求者ＩＰアドレス(4)			
サーバＩＰアドレス(4)			
リレーエージェントＩＰアドレス(4)			
クライアントMACアドレス(16)			
サーバのホスト名(64)			
ブートファイル名(128)			
オプション(可変長)			

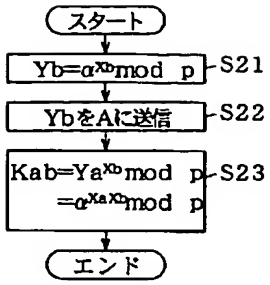
（ｂ）

・ＩＰアドレス
・ネットマスク
・デフォルトゲートウェイＩＰアドレス
・貸し出し有効期限
・ドメインネームサーバアドレス
・ドメイン名

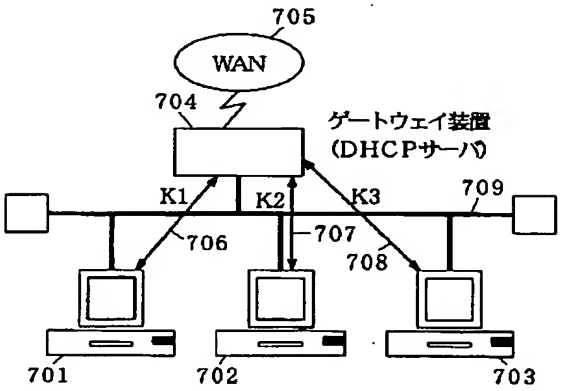
【図８】



【図７】



【図９】



【図１０】

（ａ）

MACアドレス	ＩＰアドレス	秘密鍵	共有鍵
aa.aa.aa.aa.aa.aa	192.168.0.X	Xa	K1

（ｂ）

MACアドレス	ＩＰアドレス	秘密鍵	共有鍵
aa:aa:aa:aa:aa:aa	192.168.0.X	X1	K1
yy:yy:yy:yy:yy:yy	192.168.0.b	X2	K2
zz:zz:zz:zz:zz:zz	192.168.0.c	X3	K3

フロントページの続き

Ｆターム(参考)　5J104 AA16 BA02 EA24 EA28 EA33
NA03 PA07
5K030 GA15 HD03 HD06 JT02 LD19
5K033 AA08 CB08 CC01 DB10 DB18
9A001 BB04 CC03 CC08 DD10 EE03
JJ13 JJ14 JJ25 JJ27 KK56
LL03